Terms used **tree structure casino game** Found **581** of **201,062**

Sort results by relevance Save results to a Binder Try an Advanced Search

Display results expanded form Search Tips Try this search in The ACM Guide

Open results in a new window

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next

Best 200 shown Relevance scale

1 Global Virtual Time and distributed synchronization

Jeffrey S. Steinman, Craig A. Lee, Linda F. Wilson, David M. Nicol

July 1995 **ACM SIGSIM Simulation Digest , Proceedings of the ninth workshop on Parallel and distributed simulation PADS '95**, Volume 25 Issue 1

Publisher: IEEE Computer Society, ACM Press

Full text available: pdf(1.46 MB) Publisher Site Additional Information: full citation, abstract, references, citings, index terms

Global Virtual Time (GVT) is the fundamental synchronization concept in optimistic simulations. It is defined as the earliest time tag within the set of unprocessed pending events in distributed simulation. A number of techniques for determining GVT have been proposed in recent years, each having their own intrinsic properties. However, most of these techniques either focus on specific types of simulation problems or assume specific hardware support. This paper specifically addresses the GV ...

Keywords: GVT computation, SPEEDES GVT, SPEEDES framework, Synchronous Parallel Environment for Emulation and Discrete-Event Simulation framework, digital simulation, distributed simulation, distributed synchronization, efficiency, event processing, flow control, fundamental synchronization concept, global reduction operations, global virtual time, interactive support, message passing, optimistic simulations, parallel programming, portability, real time use, real-time systems, scalability, software fault tolerance, synchronisation, unprocessed pending events

2 Special issue: Game-playing programs: theory and practice

M. A. Bramer

April 1982 **ACM SIGART Bulletin**, Issue 80

Publisher: ACM Press

Full text available: pdf(9.23 MB) Additional Information: full citation, abstract

This collection of articles has been brought together to provide SIGART members with an overview of Artificial Intelligence approaches to constructing game-playing programs. Papers on both theory and practice are included.

3 Game space design foundations for trans-reality games

Craig A. Lindley

June 2005 **Proceedings of the 2005 ACM SIGCHI International Conference on Advances in computer entertainment technology ACE '05**

Publisher: ACM Press
Full text available: pdf(409.74 KB) Additional Information: full citation, abstract, references, index terms

Trans-reality games are games that take advantage of pervasive, mobile, ubiquitous, location-based and mixed reality technical infrastructures to create game spaces that can include physical reality together with one or more virtual realities. Creating these games requires basic design decisions about the relationships between the large scale game spaces involved. In particular, the different game spaces can be related by general 3D coordinate system transforms, together with decisions regarding ...

Keywords: game space design, mixed reality games, trans-reality games

4 Wireless game and game story: Contextual information access and storytelling in mixed reality using hypermedia
Luis Romero, JORGE SANTIAGO, NUNO CORREIA
July 2004 **Computers in Entertainment (CIE)**, Volume 2 Issue 3
Publisher: ACM Press
Full text available: pdf(480.08 KB) Additional Information: full citation, abstract, references, index terms

This article describes gaming and storytelling activities in a mixed environment that integrates the real and virtual worlds, uses an augmented reality paradigm, and is supported by a structuring and presentation framework for use in context-aware mixed-reality applications. The basis of the framework is a generic hypermedia model that can handle different media elements, objects, and relations between spaces and locations in physical and virtual worlds. A main component of the model deals wi ...

Keywords: hypermedia interfaces, hypermedia model, mixed and augmented reality, mobile gaming and storytelling

5 Accordion summarization for end-game browsing on PDAs and cellular phones
Orkut Buyukkokten, Hector Garcia-Molina, Andreas Paepcke
March 2001 **Proceedings of the SIGCHI conference on Human factors in computing systems CHI '01**
Publisher: ACM Press
Full text available: pdf(909.94 KB) Additional Information: full citation, abstract, references, citings, index terms

We demonstrate a new browsing technique for devices with small displays such as PDAs or cellular phones. We concentrate on end-game browsing, where the user is close to or on the target page. We make browsing more efficient and easier by Accordion Summarization. In this technique the Web page is first represented as a short summary. The user can then drill down to discover relevant parts of the page. If desired, keywords can be highlighted and exposed automatically. We discuss our technique ...

Keywords: HTML, PDA (Personal Digital Assistant), WAP, WML, WWW (World-Wide Web)

6 Storytelling: Believable environments: generating interactive storytelling in vast location-based pervasive games
Anton Gustafsson, John Bichard, Liselott Brunnberg, Oskar Juhlin, Marco Combetto
June 2006 **Proceedings of the 2006 ACM SIGCHI international conference on Advances in computer entertainment technology ACE '06**
Publisher: ACM Press
Full text available: pdf(239.21 KB) Additional Information: full citation, abstract, references, index terms

Generating content into vast areas is a relevant challenge in the field of location-based pervasive games. In this paper, we present a game prototype that enables children travelling in the back seat of a car to enjoy a narrated experience where gameplay combines with the experience of traveling through the road network. The prototype is designed to provide what we refer to as a believable environment. We propose four design characteristics to persuasively include a journey within a pervasive ga ...

Keywords: audio centric, backseat playground, believable environment, interactive storytelling, location based, pervasive game, prototype performance test

7 Morphological study of the video games

Julian Alvarez, Damien Djaouti, Rashid Ghassempouri, Jean-Pierre Jessel, Gilles Methel

December 2006 **Procedings of the 3rd Australasian conference on Interactive entertainment IE '06**

Publisher: Murdoch University

Full text available: pdf(605.27 KB) Additional Information: full citation, abstract, references, index terms

The aim of this article is first to present V.E.Ga.S., a tool which intend to classify video games, study their nature and to corroborate hypothesis by a pragmatic approach. It consists in studying a significant number of video games in order to index their composition of elementary "game bricks". Basing our study on this bricks and crossing them, we try to classify and study video games. In a second time, this paper presents the classification deduced from the results of V.E.Ga.S.

Keywords: bricks, experimental methods, game design, gameplay, morphology, taxonomy, video games

8 Session 3: Computing approximate bayes-nash equilibria in tree-games of incomplete information

Satinder Singh, Vishal Soni, Michael Wellman

May 2004 **Proceedings of the 5th ACM conference on Electronic commerce EC '04**

Publisher: ACM Press

Full text available: pdf(392.84 KB) Additional Information: full citation, abstract, references, citings, index terms

We provide efficient algorithms for finding approximate Bayes-Nash equilibria (BNE) in graphical, specifically tree, games of incomplete information. In such games an agent's payoff depends on its private type as well as on the actions of the agents in its local neighborhood in the graph. We consider two classes of such games: (1) arbitrary tree-games with discrete types, and (2) tree-games with continuous types but with constraints on the effect of type on payoffs. For each class we present a m ...

Keywords: approximate bayes-nash equilibria, games of incomplete information, structured games

9 Multi-agent reinforcement learning: Multi-agent learning in extensive games with complete information

Pu Huang, Katia Sycara

July 2003 **Proceedings of the second international joint conference on Autonomous agents and multiagent systems AAMAS '03**

Publisher: ACM Press

Full text available: pdf(347.73 KB) Additional Information: full citation, abstract, references, index terms

Learning in a multi-agent system is difficult because the learning environment jointly created by all learning agents is *time-variant*. This paper studies the model of multi-agent learning in complete-information extensive games (CEGs). We provide two provably convergent algorithms for this model. Both algorithms utilize the special structure of CEGs and guarantee both individual and collective convergence. Our work contributes to the multi-agent learning literature in several aspects: 1. ...

Keywords: extensive games, learning, multi-agent systems

10 Contributed session 5: Pure Nash equilibria: hard and easy games

Georg Gottlob, Gianluigi Greco, Francesco Scarcello
June 2003 **Proceedings of the 9th conference on Theoretical aspects of rationality and knowledge TARK '03**
Publisher: ACM Press

Full text available: pdf(1.34 MB) Additional Information: full citation, abstract, references, citings, index terms

In this paper we investigate complexity issues related to pure Nash equilibria of strategic games. We show that, even in very restrictive settings, determining whether a game has a pure Nash Equilibrium is NP-hard, while deciding whether a game has a strong Nash equilibrium is Σ^P_2-complete. We then study practically relevant restrictions that lower the complexity. In particular, we are interested in quantitative and qualitative restrictions of the way each play ...

11 Correlated equilibria in graphical games

Sham Kakade, Michael Kearns, John Langford, Luis Ortiz
June 2003 **Proceedings of the 4th ACM conference on Electronic commerce EC '03**
Publisher: ACM Press

Full text available: pdf(178.85 KB) Additional Information: full citation, abstract, references, citings, index terms

We examine correlated equilibria in the recently introduced formalism of graphical games, a succinct representation for multiplayer games. We establish a natural and powerful relationship between the graphical structure of a multiplayer game and a certain Markov network representing distributions over joint actions. Our first main result establishes that this Markov network succinctly represents all correlated equilibria of the graphical game up to expected payoff equivalence. Our second main re ...

Keywords: correlated equilibria, game theory, graphical games, graphical models

12 Playing large games using simple strategies

Richard J. Lipton, Evangelos Markakis, Aranyak Mehta
June 2003 **Proceedings of the 4th ACM conference on Electronic commerce EC '03**
Publisher: ACM Press

Full text available: pdf(186.64 KB) Additional Information: full citation, abstract, references, citings, index terms

We prove the existence of ε-Nash equilibrium strategies with support logarithmic in the number of pure strategies. We also show that the payoffs to all players in any (exact) Nash equilibrium can be ε-approximated by the payoffs to the players in some such logarithmic support ε-Nash equilibrium. These strategies are also uniform on a multiset of logarithmic size and therefore this leads to a quasi-polynomial algorithm for computing an ε-Nash equilibrium. To our knowledge this ...

Keywords: nash equilibrium, probabilistic method

13 Session 5: P2P and streaming: Provisioning on-line games: a traffic analysis of a busy counter-strike server

Wu-chang Feng, Francis Chang, Wu-chi Feng, Jonathan Walpole

November 2002 **Proceedings of the 2nd ACM SIGCOMM Workshop on Internet measurment IMW '02**

Publisher: ACM Press

Full text available: pdf(496.06 KB) Additional Information: full citation, abstract, references, citings, index terms

This paper describes the results of a 500 million packet trace of a popular on-line, multi-player, game server. The results show that the traffic behavior of this heavily loaded game server is highly predictable and can be attributed to the fact that current game designs target the *saturation of the narrowest, last-mile link*. Specifically, in order to maximize the interactivity of the game and to provide relatively uniform experiences between all players, on-line games typically fix their ...

14 Fast algorithms for finding randomized strategies in game trees

Daphne Koller, Nimrod Megiddo, Bernhard von Stengel

May 1994 **Proceedings of the twenty-sixth annual ACM symposium on Theory of computing STOC '94**

Publisher: ACM Press

Full text available: pdf(1.09 MB) Additional Information: full citation, references, citings, index terms

15 Exploring the use of ray tracing for future games

Heiko Friedrich, Johannes Günther, Andreas Dietrich, Michael Scherbaum, Hans-Peter Seidel, Philipp Slusallek

July 2006 **Proceedings of the 2006 ACM SIGGRAPH symposium on Videogames sandbox '06**

Publisher: ACM Press

Full text available: pdf(544.46 KB) Additional Information: full citation, abstract, references, index terms

Rasterization hardware and computer games have always been tightly connected: The hardware implementation of rasterization has made complex interactive 3D games possible while requirements for future games drive the development of increasingly parallel GPUs and CPUs. Interestingly, this development - together with important algorithmic improvements - also enabled *ray tracing* to achieve realtime performance recently.In this paper we explore the opportunities offered by ray tracing based ga ...

Keywords: dynamic scenes, games development, global illumination, graphics hardware, realtime ray tracing, simulation

16 Game: A component based architecture for distributed, pervasive gaming applications

Carsten Magerkurth, Timo Engelke, Dan Grollman

June 2006 **Proceedings of the 2006 ACM SIGCHI international conference on Advances in computer entertainment technology ACE '06**

Publisher: ACM Press

Full text available: pdf(326.31 KB) Additional Information: full citation, abstract, references, index terms

In this paper, we describe a component based architecture for developing distributed,

pervasive games that integrate tangible and graphical user interface components. We first discuss some of the interface components we have developed and then present a coordination infrastructure called Pegasus that allows flexibly coupling and reconfiguring components during runtime. On top of Pegasus we have created a language for describing pervasive games called DHG and briefly present a first sample applic ...

Keywords: TUI, computer games, entertainment, hybrid environments, pervasive games, tabletop games, tangible interfaces

17 Workshop papers: Game theory perspectives on client: vendor relationships in offshore software outsourcing

Nilay V. Oza

May 2006 **Proceedings of the 2006 international workshop on Economics driven software engineering research EDSER '06**

Publisher: ACM Press

Full text available: pdf(84.45 KB) Additional Information: full citation, abstract, references, index terms

The objective of this paper is to provide the initial literature based insights into the game theory specifically with the viewpoint of client - vendor relationships in offshore software outsourcing. Game theory has been used for long in understanding various contexts in economics and other disciplines. Offshore software outsourcing relates to the situation in which client and vendor are operating from different countries. Subsequently, in this paper, the initial understanding of game theory foc ...

Keywords: economics, game theory, software engineering, software outsourcing

18 Computing pure nash equilibria in graphical games via markov random fields

Constantinos Daskalakis, Christos H. Papadimitriou

June 2006 **Proceedings of the 7th ACM conference on Electronic commerce EC '06**

Publisher: ACM Press

Full text available: pdf(159.77 KB) Additional Information: full citation, abstract, references, index terms

We present a reduction from graphical games to Markov random fields so that pure Nash equilibria in the former can be found by statistical inference on the latter. Our result, when combined with the junction tree algorithm for statistical inference, yields a unified proof of all previously known tractable cases of the NP-complete problem of finding pure Nash equilibria in graphical games, but also implies efficient algorithms for new classes, such as the games with $O(\log n)$ treewid ...

Keywords: markov random fields, nash equilibrium, treewidth

19 A traffic characterization of popular on-line games

Wu-chang Feng, Francis Chang, Wu-chi Feng, Jonathan Walpole

June 2005 **IEEE/ACM Transactions on Networking (TON)**, Volume 13 Issue 3

Publisher: IEEE Press

Full text available: pdf(1.42 MB) Additional Information: full citation, abstract, references, citings, index terms

This paper describes the results of the first comprehensive analysis of a range of popular on-line, multiplayer, game servers. The results show that the traffic behavior of these servers is highly predictable and can be attributed to the fact that current game designs target the saturation of the narrowest, last-mile link. Specifically, in order to maximize the interactivity of the game itself and to provide relatively uniform experiences between players playing over different network speeds, on ...

Keywords: communication system traffic, games, measurement, network servers, networks

20 Robot's play: interactive games with sociable machines

Andrew G. Brooks, Jesse Gray, Guy Hoffman

September 2004 **Proceedings of the 2004 ACM SIGCHI International Conference on Advances in computer entertainment technology ACE '04**

Publisher: ACM Press

Full text available: pdf(284.22 KB) Additional Information: full citation, abstract, references, citings

Personal robots for human entertainment form a new class of computer-based entertainment that is beginning to become commercially and computationally practical. We expect a principal manifestation of their entertainment capabilities will be socially interactive game playing. We describe this form of gaming and summarize our current efforts in this direction on our lifelike, expressive, autonomous humanoid robot. Our focus is on teaching the robot via playful interaction using natural social gest ...

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next

Terms used **preimage casino game** Found **36** of **201,062**

Sort results by: relevance
Display results: expanded form
Save results to a Binder
Search Tips
Open results in a new window
Try an Advanced Search
Try this search in The ACM Guide

Results 1 - 20 of 36 Result page: **1** 2 next

Relevance scale

1 1 - Regular Articles: A performance study of data layout techniques for improving data locality in refinement-based pathfinding
Robert Niewiadomski, José Nelson Amaral, Robert C. Holte
December 2004 **Journal of Experimental Algorithmics (JEA)**, Volume 9
Publisher: ACM Press
Full text available: pdf(1.46 MB) Additional Information: full citation, abstract, references, citings, index terms

The widening gap between processor speed and memory latency increases the importance of crafting data structures and algorithms to exploit temporal and spatial locality. Refinement-based pathfinding algorithms, such as Classic Refinement (CR), find quality paths in very large sparse graphs where traditional search techniques fail to generate paths in acceptable time. In this paper, we present a performance evaluation study of three simple data structure transformations aimed at improving the dat ...

Keywords: Cache-conscious algorithms, classical refinement, pathfinding

2 Witness indistinguishable and witness hiding protocols
U. Feige, A. Shamir
April 1990 **Proceedings of the twenty-second annual ACM symposium on Theory of computing STOC '90**
Publisher: ACM Press
Full text available: pdf(1.11 MB) Additional Information: full citation, citings, index terms

3 Using smartcards to secure a personalized gambling device
William A. Aiello, Aviel D. Rubin, Martin J. Strauss
November 1999 **Proceedings of the 6th ACM conference on Computer and communications security CCS '99**
Publisher: ACM Press
Full text available: pdf(762.94 KB) Additional Information: full citation, abstract, references, index terms

We introduce a technique for using an untrusted device, such as a hand-held personal digital assistant or a laptop to perform real financial transactions without a network. We utilize the tamper-resistant nature of smartcards to store value on them and perform probabilistic computations based on user input. We discuss an application of this to gambling. The technique has the properties that the user is guaranteed to make money

when he wins and the house is guaranteed to make money w ...

4 Public-key cryptography and password protocols

Shai Halevi, Hugo Krawczyk

August 1999 **ACM Transactions on Information and System Security (TISSEC)**, Volume 2 Issue 3

Publisher: ACM Press

Full text available: pdf(275.84 KB) Additional Information: full citation, abstract, references, citings, index terms, review

We study protocols for strong authentication and key exchange in asymmetric scenarios where the authentication server possesses ~a pair of private and public keys while the client has only a weak human-memorizable password as its authentication key. We present and analyze several simple password authentication protocols in this scenario, and show that the security of these protocols can be formally proven based on standard cryptographic assumptions. Remarkably, our analysis shows optimal re ...

Keywords: dictionary attacks, hand-held certificates, key exchange, passwords, public passwords, public-key protocols

5 Session 8A: Non-interactive and reusable non-malleable commitment schemes

Ivan Damgard, Jens Groth

June 2003 **Proceedings of the thirty-fifth annual ACM symposium on Theory of computing STOC '03**

Publisher: ACM Press

Full text available: pdf(333.10 KB) Additional Information: full citation, abstract, references, citings, index terms

We consider non-malleable (NM) and universally composable (UC) commitment schemes in the common reference string (CRS) model. We show how to construct non-interactive NM commitments that remain non-malleable even if the adversary has access to an arbitrary number of commitments from honest players - rather than one, as in several previous schemes. We show this is a strictly stronger security notion. Our construction is the first non-interactive scheme achieving this that can be based on the mini ...

Keywords: commitment, non-malleability, one-way function, signature, universal composability

6 Secure distributed human computation

Craig Gentry, Zulfikar Ramzan, Stuart Stubblebine

June 2005 **Proceedings of the 6th ACM conference on Electronic commerce EC '05**

Publisher: ACM Press

Full text available: pdf(257.80 KB) Additional Information: full citation, abstract, references, index terms

This paper is a preliminary exploration of secure distributed *human* computation. We consider the general paradigm of using large-scale distributed computation to solve difficult problems, but where humans can act as agents and provide candidate solutions. We are especially motivated by problem classes that appear to be difficult for computers to solve effectively, but are easier for humans; e.g., image analysis, speech recognition, and natural language processing. This paradigm already se ...

Keywords: B24b, human distributed computation

7 Session 10B: Lower-stretch spanning trees

Michael Elkin, Yuval Emek, Daniel A. Spielman, Shang-Hua Teng
May 2005 **Proceedings of the thirty-seventh annual ACM symposium on Theory of computing STOC '05**
Publisher: ACM Press

Full text available: pdf(221.55 KB) Additional Information: full citation, abstract, references, citings, index terms

We show that every weighted connected graph G contains as a subgraph a spanning tree into which the edges of G can be embedded with average stretch $O(\log^2 n \log \log n)$. Moreover, we show that this tree can be constructed in time $O(m \log^2 n)$ in general, and in time $O(m \log n)$ if the input graph is unweighted. The main ingredient in our construction is a novel graph decomposition technique.Our new a ...

Keywords: low-distortion embeddings, low-stretch spanning trees, probabilistic tree metrics

8 Applied cryptography: Reusable cryptographic fuzzy extractors
Xavier Boyen
October 2004 **Proceedings of the 11th ACM conference on Computer and communications security CCS '04**
Publisher: ACM Press

Full text available: pdf(251.61 KB) Additional Information: full citation, abstract, references, citings, index terms

We show that a number of recent definitions and constructions of fuzzy extractors are not adequate for multiple uses of the same fuzzy secret---a major shortcoming in the case of biometric applications. We propose two particularly stringent security models that specifically address the case of fuzzy secret reuse, respectively from an outsider and an insider perspective, in what we call a chosen perturbation attack. We characterize the conditions that fuzzy extractors need to satisfy to be sec ...

Keywords: biometric keying, chosen perturbation security, fuzzy extractor, zero storage biometric authentication

9 Software protection and simulation on oblivious RAMs
Oded Goldreich, Rafail Ostrovsky
May 1996 **Journal of the ACM (JACM)**, Volume 43 Issue 3
Publisher: ACM Press

Full text available: pdf(3.44 MB) Additional Information: full citation, abstract, references, citings, index terms

Software protection is one of the most important issues concerning computer practice. There exist many heuristics and ad-hoc methods for protection, but the problem as a whole has not received the theoretical treatment it deserves. In this paper, we provide theoretical treatment of software protection. We reduce the problem of software protection to the problem of efficient simulation on oblivious RAM.A machine is oblivious if thhe sequence in wh ...

Keywords: pseudorandom functions, simulation of random access machines, software protection

10 Some facets of complexity theory and cryptography: A five-lecture tutorial
Jörg Rothe
December 2002 **ACM Computing Surveys (CSUR)**, Volume 34 Issue 4

Publisher: ACM Press

Full text available: pdf(2.78 MB) Additional Information: full citation, abstract, references, citings, index terms, review

In this tutorial, selected topics of cryptology and of computational complexity theory are presented. We give a brief overview of the history and the foundations of classical cryptography, and then move on to modern public-key cryptography. Particular attention is paid to cryptographic protocols and the problem of constructing key components of protocols such as one-way functions. A function is one-way if it is easy to compute, but hard to invert. We discuss the notion of one-way functions both ...

Keywords: Complexity theory, interactive proof systems, one-way functions, public-key cryptography, zero-knowledge protocols

11 Session 8B: Universally composable two-party and multi-party secure computation

Ran Canetti, Yehuda Lindell, Rafail Ostrovsky, Amit Sahai

May 2002 **Proceedings of the thiry-fourth annual ACM symposium on Theory of computing STOC '02**

Publisher: ACM Press

Full text available: pdf(250.32 KB) Additional Information: full citation, abstract, references, citings, index terms

We show how to securely realize any multi-party functionality in a *universally composable* way, regardless of the number of corrupted participants. That is, we consider a multi-party network with open communication and an adversary that can adaptively corrupt as many parties as it wishes. In this setting, our protocols allow any subset of the parties (with pairs of parties being a special case) to securely realize any desired functionality of their local inputs, and be guaranteed that secu ...

12 Harold: a world made of drawings

Jonathan M. Cohen, John F. Hughes, Robert C. Zeleznik

June 2000 **Proceedings of the 1st international symposium on Non-photorealistic animation and rendering NPAR '00**

Publisher: ACM Press

Full text available: pdf(1.97 MB) Additional Information: full citation, references, citings, index terms

Keywords: billboards, gestural interfaces, scene description, stroke-based rendering

13 Asymmetric fingerprinting for larger collusions

Birgit Pfitzmann, Michael Waidner

April 1997 **Proceedings of the 4th ACM conference on Computer and communications security CCS '97**

Publisher: ACM Press

Full text available: pdf(1.37 MB) Additional Information: full citation, references, citings, index terms

14 Revealing information while preserving privacy

Irit Dinur, Kobbi Nissim

June 2003 **Proceedings of the twenty-second ACM SIGMOD-SIGACT-SIGART symposium on Principles of database systems PODS '03**

Publisher: ACM Press

Full text available: pdf(209.90 KB) Additional Information: full citation, abstract, references, citings, index

terms

We examine the tradeoff between privacy and usability of statistical databases. We model a statistical database by an n-bit string $d1,..,dn$, with a query being a subset $q \subseteq [n]$ to be answered by $\Sigma i \in q\ di$. Our main result is a polynomial reconstruction algorithm of data from noisy (perturbed) subset sums. Applying this reconstruction algorithm to statistical database ...

Keywords: data reconstruction, integrity and security, subset-sums with noise

15 Session 2B: Black-box constructions for secure computation

Yuval Ishai, Eyal Kushilevitz, Yehuda Lindell, Erez Petrank

May 2006 **Proceedings of the thirty-eighth annual ACM symposium on Theory of computing STOC '06**

Publisher: ACM Press

Full text available: pdf(269.51 KB) Additional Information: full citation, abstract, references, index terms

It is well known that the secure computation of non-trivial functionalities in the setting of no honest majority requires computational assumptions. We study the way such computational assumptions are used. Specifically, we ask whether the secure protocol can use the underlying primitive (e.g., one-way trapdoor permutation) in a *black-box* way, or must it be *nonblack-box* (by referring to the code that computes this primitive)? Despite the fact that many general constructions of cry ...

Keywords: black-box reductions, oblivious transfer, secure computation, theory of cryptography

16 Distributed computing: ACM SIGACT news distributed computing column 24

Sergio Rajsbaum

December 2006 **ACM SIGACT News**, Volume 37 Issue 4

Publisher: ACM Press

Full text available: pdf(528.05 KB) Additional Information: full citation, abstract, references

The Distributed Computing Column covers the theory of systems that are composed of a number of interacting computing elements. These include problems of communication and networking, databases, distributed shared memory, multiprocessor architectures, operating systems, verification, Internet, and the Web. This issue consists of:• "Security and Composition of Cryptographic Protocols: A Tutorial (Part II)" by Ran Canetti.The first part appeared in the previous SIGACT News, the September 2006 ...

17 A complete problem for statistical zero knowledge

Amit Sahai, Salil Vadhan

March 2003 **Journal of the ACM (JACM)**, Volume 50 Issue 2

Publisher: ACM Press

Full text available: pdf(397.62 KB) Additional Information: full citation, abstract, references, citings, index terms

We present the first complete problem for SZK, the class of promise problems possessing statistical zero-knowledge proofs (against an honest verifier). The problem, called Statistical Difference, is to decide whether two efficiently samplable distributions are either statistically close or far apart. This gives a new characterization of SZK that makes *no reference to interaction or zero knowledge*.We propose the use of complete problems to unify and extend the study of statistical zero kno ...

Keywords: Knowledge complexity, proof systems, statistical difference, zero knowledge

18 A Web Odyssey: from Codd to XML

Victor Vianu

May 2001 **Proceedings of the twentieth ACM SIGMOD-SIGACT-SIGART symposium on Principles of database systems PODS '01**

Publisher: ACM Press

Full text available: pdf(282.10 KB) Additional Information: full citation, references, citings, index terms

19 Information retrieval as statistical translation

Adam Berger, John Lafferty

August 1999 **Proceedings of the 22nd annual international ACM SIGIR conference on Research and development in information retrieval SIGIR '99**

Publisher: ACM Press

Full text available: pdf(284.31 KB) Additional Information: full citation, references, citings, index terms

20 Evolutionary multiobjective optimization: papers: On the effect of populations in evolutionary multi-objective optimization

Oliver Giel, Per Kristian Lehre

July 2006 **Proceedings of the 8th annual conference on Genetic and evolutionary computation GECCO '06**

Publisher: ACM Press

Full text available: pdf(217.69 KB) Additional Information: full citation, abstract, references, index terms

Multi-objective evolutionary algorithms (MOEAs) have become increasingly popular as multi-objective problem solving techniques. An important open problem is to understand the role of populations in MOEAs. We present a simple bi-objective problem which emphasizes when populations are needed. Rigorous runtime analysis point out an exponential runtime gap between the population-based algorithm *Simple Evolutionary Multi-objective Optimizer* (SEMO) and several single individual-based algorithms ...

Keywords: evolutionary algorithms, multi-objective optimization, runtime analysis

Results 1 - 20 of 36 Result page: **1** 2 next

Results for "((preimage<in>metadata) <and> (game<in>metadata))<or> (casino<in&g..." e-mail
Your search matched **2** of **446532** documents.
A maximum of **100** results are displayed, **25** to a page, sorted by **Relevance** in **Descending** order.

» Search Options

View Session History

New Search

Modify Search

((preimage<in>metadata) <and> (game<in>metadata))<or> (casino<in>metadata Search

Check to search only within this results set

Display Format: Citation Citation & Abstract

» Key

IEEE JNL	IEEE Journal or Magazine
IET JNL	IET Journal or Magazine
IEEE CNF	IEEE Conference Proceeding
IET CNF	IET Conference Proceeding
IEEE STD	IEEE Standard

view selected items Select All Deselect All

1. **News Briefs**
Paulson, L.D.;
Computer
Volume 38, Issue 4, April 2005 Page(s):24 - 26
Digital Object Identifier 10.1109/MC.2005.135
Full Text: PDF(216 KB) IEEE JNL
Rights and Permissions

2. **Parallelism speeds data mining**
Reese Hedberg, S.;
Parallel & Distributed Technology: Systems & Applications, IEEE [see also IEE
Volume 3, Issue 4, Winter 1995 Page(s):3 - 6
Digital Object Identifier 10.1109/88.473600
AbstractPlus | Full Text: PDF(392 KB) IEEE JNL
Rights and Permissions

Results for "(('tree structure'<in>metadata) <and> (game<in>metadata))" e-mail
Your search matched 0 documents.
A maximum of 100 results are displayed, 25 to a page, sorted by Relevance in Descending order.

» Search Options

View Session History

New Search

Modify Search

(('tree structure'<in>metadata) <and> (game<in>metadata)) Search

Check to search only within this results set

Display Format: Citation Citation & Abstract

» Key

IEEE JNL	IEEE Journal or Magazine
IET JNL	IET Journal or Magazine
IEEE CNF	IEEE Conference Proceeding
IET CNF	IET Conference Proceeding
IEEE STD	IEEE Standard

No results were found.

Please edit your search criteria and try again. Refer to the Help pages if you need assistan search.

Web Results **1 - 10** of about **80** for **"tree structure", "preimage", game**. (**0.41** seconds)

[PDF] Herding Hash Functions and the Nostradamus Attack
File Format: PDF/Adobe Acrobat - View as HTML
The herding attack shows that the CTFP **preimage** resistance of a hash ... sions into a **tree structure**. Figure 3.1 describes the basic idea: Note that edges ...
csrc.nist.gov/pki/HashWorkshop/2005/Oct31_Presentations/Kelsey_HerdingHash.pdf - Similar pages

Low-overhead secure information processing for mobile gaming and ...
The **game** may be characterized by a player **game tree structure** associated with ... let another decision **preimage** mean "do not link with the next **game** node. ...
www.freepatentsonline.com/20020147044.html - 80k - Cached - Similar pages

[PDF] Herding Hash Functions and the Nostradamus Attack
File Format: PDF/Adobe Acrobat - View as HTML
The herding attack shows that the CTFP **preimage** resistance of a hash function like MD5 or ... builds the **tree structure** during the collision search. ...
eprint.iacr.org/2005/281.pdf - Similar pages

[PDF] Herding Hash Functions and the Nostradamus Attack
File Format: PDF/Adobe Acrobat - View as HTML
The herding attack shows that the CTFP **preimage** resistance of a hash ... then searching for collisions, the attacker dynamically builds the **tree structure** ...
www.cs.washington.edu/homes/yoshi/papers/EC06/herding.pdf - Similar pages

[PDF] Microsoft PowerPoint - preneel_wcap06v1.ppt
File Format: PDF/Adobe Acrobat - View as HTML
take a **preimage** resistant hash function; add an input bit b and replace one ... z = result of all Australia cricket **games** between 2010 and 2020 ...
homes.esat.kuleuven.be/~preneel/preneel_hash_wcap06.pdf - Similar pages

[PDF] Herding Hash Functions and the Nostradamus Attack
File Format: PDF/Adobe Acrobat - View as HTML
hash functions should have–Chosen Target Forced Prefix (CTFP) **preimage** ... Alice and Bob want to agree on a shared random sequence for some **game**. ...
mirror.cr.yp.to/eprint.iacr.org/2005/281.pdf - Supplemental Result - Similar pages

[PDF] LNCS 3329 - Higher Order Universal One-Way Hash Functions
File Format: PDF/Adobe Acrobat
that it is hard to find a second **preimage**. First a challenge input is selected ... The second type has a **tree structure**. Here the two constructions with a ...
www.springerlink.com/index/67MFJA1CLVLTXXVA.pdf - Similar pages

[PDF] PII: 0166-218X(91)90086-C
File Format: PDF/Adobe Acrobat - View as HTML
treap, namely the **tree structure** obtained by inser- ... chance of computing the **preimage** f-'(y) for a randomly chosen element y. ...
www.student.cs.uwaterloo.ca/~cs466/Old_courses/F06/Karp.pdf - Similar pages

[PS] The Dining Cryptographers in the Disco: Unconditional Sender and ...
File Format: Adobe PostScript - View as Text

One way is to form a global **tree structure** like that in [Merk_88]. ... Silvio Micali, Avi Wigderson: How to play any mental **game** - or - a ...
www.semper.org/sirene/publ/WaPf1_89DiscoEngl.ps.gz - Similar pages

[PDF] KASER: Knowledge Amplification by Structured Expert Randomization
File Format: PDF/Adobe Acrobat
"VEHICLE"). KASER's make use of a dynamic **tree structure**, ... The problem is that the **preimage** of a typical. goal state cannot be effectively constrained ...
ieeexplore.ieee.org/iel5/3477/29778/01356021.pdf - Similar pages

Result Page: 1 2 3 4 5 6 7 8 **Next**

"tree structure", "preimage", game Search

Search within results | Language Tools | Search Tips | Dissatisfied? Help us improve

---

Web Results **1** - **10** of about **80** for **"tree structure", "preimage", game**. (**0.41** seconds)

[PDF] Herding Hash Functions and the Nostradamus Attack
File Format: PDF/Adobe Acrobat - View as HTML
The herding attack shows that the CTFP **preimage** resistance of a hash ... sions into a **tree structure**. Figure 3.1 describes the basic idea: Note that edges ...
csrc.nist.gov/pki/HashWorkshop/2005/Oct31_Presentations/Kelsey_HerdingHash.pdf - Similar pages

Low-overhead secure information processing for mobile gaming and ...
The **game** may be characterized by a player **game tree structure** associated with ... let another decision **preimage** mean "do not link with the next **game** node. ...
www.freepatentsonline.com/20020147044.html - 80k - Cached - Similar pages

[PDF] Herding Hash Functions and the Nostradamus Attack
File Format: PDF/Adobe Acrobat - View as HTML
The herding attack shows that the CTFP **preimage** resistance of a hash function like MD5 or ... builds the **tree structure** during the collision search. ...
eprint.iacr.org/2005/281.pdf - Similar pages

[PDF] Herding Hash Functions and the Nostradamus Attack
File Format: PDF/Adobe Acrobat - View as HTML
The herding attack shows that the CTFP **preimage** resistance of a hash ... then searching for collisions, the attacker dynamically builds the **tree structure** ...
www.cs.washington.edu/homes/yoshi/papers/EC06/herding.pdf - Similar pages

[PDF] Microsoft PowerPoint - preneel_wcap06v1.ppt
File Format: PDF/Adobe Acrobat - View as HTML
take a **preimage** resistant hash function; add an input bit b and replace one ... z = result of all Australia cricket **games** between 2010 and 2020 ...
homes.esat.kuleuven.be/~preneel/preneel_hash_wcap06.pdf - Similar pages

[PDF] Herding Hash Functions and the Nostradamus Attack
File Format: PDF/Adobe Acrobat - View as HTML
hash functions should have–Chosen Target Forced Prefix (CTFP) **preimage** ... Alice and Bob want to agree on a shared random sequence for some **game**. ...
mirror.cr.yp.to/eprint.iacr.org/2005/281.pdf - Supplemental Result - Similar pages

[PDF] LNCS 3329 - Higher Order Universal One-Way Hash Functions
File Format: PDF/Adobe Acrobat
that it is hard to find a second **preimage**. First a challenge input is selected ... The second type has a **tree structure**. Here the two constructions with a ...
www.springerlink.com/index/67MFJA1CLVLTXXVA.pdf - Similar pages

[PDF] PII: 0166-218X(91)90086-C
File Format: PDF/Adobe Acrobat - View as HTML
treap, namely the **tree structure** obtained by inser- ... chance of computing the **preimage** f-'(y) for a randomly chosen element y. ...
www.student.cs.uwaterloo.ca/~cs466/Old_courses/F06/Karp.pdf - Similar pages

[PS] The Dining Cryptographers in the Disco: Unconditional Sender and ...
File Format: Adobe PostScript - View as Text

One way is to form a global **tree structure** like that in [Merk_88]. ... Silvio Micali, Avi Wigderson: How to play any mental **game** - or - a ...
www.semper.org/sirene/publ/WaPf1_89DiscoEngl.ps.gz - Similar pages

[PDF] KASER: Knowledge Amplification by Structured Expert Randomization
File Format: PDF/Adobe Acrobat
"VEHICLE"). KASER's make use of a dynamic **tree structure**, ... The problem is that the **preimage** of a typical. goal state cannot be effectively constrained ...
ieeexplore.ieee.org/iel5/3477/29778/01356021.pdf - Similar pages

Result Page: 1 2 3 4 5 6 7 8 **Next**

"tree structure", "preimage", game Search

Search within results | Language Tools | Search Tips | Dissatisfied? Help us improve

---